Office of the State Public Defender
Administrative Policies

Subject: Mobile Devices and Services	**Policy No.: 225**
Title	**Pages: 4**
Section:	**Last Review Date: 4/11/19**
Effective Date: 11/10/10	**Revision Date: 6/10/19**

1. POLICY

The Office of the State Public Defender supports and encourages the use of personal mobile devices for employees who use these devices to enhance productivity or who are required to use a mobile device in conjunction with their job duties. Using a personal mobile device is cost-effective and, through the use of Mobile Device Management (MDM), effectively secures State data and resources at the same time. Users are responsible for securing their personal mobile device so that others cannot use it inappropriately to access State data. MDM is required on all mobile devices that access State email.

2. REQUIREMENTS FOR ISSUING A STATE DEVICE

State mobile devices shall be issued on a case by case basis with the approval of the program manager or designee. The employee will be required to sign the Mobile Device Management User Agreement required by the Department of Administration (Attachment A).

2.1 All users will be required to maintain a personal Apple or Google account (based on phone type) with recovery options.

2..2 Prior to terminating employment or returning the device, the user is required to sign out of the personal account on the device.

3. REQUIREMENTS FOR REIMBURSEMENT OF PRIVATE DEVICE COSTS

If a private device is used for business purposes a reimbursement request may be made per Attachment A, and the employee will be required to sign the Mobile Device Management User Agreement.

4. CROSS REFERENCE GUIDE

The use of mobile devices for state government work is also governed by the following policies and laws: Electronic Mail, Information Security, and Social Media found on the MOM website at http://mom.mt.gov; and 2-15-114 and 2-17-534, MCA. For a definition of a mobile device, refer to the Enterprise Mobile Device Management Policy - Section VI Definitions Mobile Device Management (MDM).

5. CLOSING

This policy shall be followed unless it conflicts with negotiated labor contracts or specific statutes, which shall take precedence to the extent applicable.

Questions about this policy can be directed to your supervisor or to:

Office of the State Public Defender, Central Services Division
44 West Park
Butte, MT 59701
(406) 496-6080

Mobile Device Management User Agreement

This User Agreement covers the use of all mobile devices that interact with State of Montana information technology resources.

Users utilizing an MDM-enrolled device acknowledge and agree:

1. The State Information Technology Services Division (SITSD) may remove State data from my enrolled mobile device, **STATE OR PERSONAL**, without any notification, resulting in loss of all State data on the enrolled mobile device. Devices enrolled as "Bring Your Own Device" (BYOD) will only experience data removal of State data. State-owned devices may be set back to factory default settings. SITSD will make a reasonable effort to contact the user in a timely manner to inform them of and reasons for the data removal. Some of the common reasons to remove State data from a mobile device are listed below:
    a. If the mobile device is suspected of being compromised and poses a threat to the State;
    b. If the mobile device user violates State policies or statutes concerning the use of the mobile device;
    c. If a technical issue arises requiring the mobile device to be wiped to resolve; or
    d. If the owner of the mobile device resigns, is terminated, or suspended with/without pay.

2. During the initial enrollment with the MDM infrastructure, default Security Profiles will be pushed to the enrolled mobile device. Security Profiles are meant to protect and secure the State's information on the mobile device. BYOD profiles are minimal and intended to only protect State data. No personal private information is collected with BYOD enrollment.

3. The Security Profiles may change because they are periodically reviewed. SITSD will attempt to inform users before changes are made, but in the case of an emergency change, prior contact may not be possible.

4. If a mobile device configured to connect to State information technology resources is lost, the user shall take the actions listed below as soon as possible, but no later than 24 hours from losing the managed mobile device:
    a. Contact the Department of Administration Security Officer and SITSD Service Desk to report the loss;
    b. Contact the cellular company that provides their service and have the mobile device deactivated; and
    c. Change their Active Directory password, which is the password associated with the user's C# which allows them access to the State network.

5. Support of the mobile device is provided by the employee's mobile device provider.

6. The use of mobile devices for state government work is also governed by the following policies and laws: Electronic Mail, Information Security, and Social Media found on the MOM website at http://mom.mt.gov; and 2-15-114 and 2-17-534, MCA. For a definition of a mobile device, refer to the Enterprise Mobile Device Management Policy - Section VI Definitions Mobile Device Management (MDM).

7. State-Owned Devices: All network activity conducted while doing State business and with State-owned resources and/or hardware is the State's property. The State reserves the right to monitor and log all State network activity including email, text messages, Twitter messages, internet use, and all other social media use, with or without notice. Therefore, there is no expectation of privacy in the use of these resources and the content of the messages sent using these resources.

   Employee-Owned Devices: The foregoing does not apply to use of employee-owned devices that do not connect to the State network. However, messages or other data content generated from such use and involving State business may be public information under Montana's open records laws and therefore subject to disclosure. In addition, each employee is responsible to identify and retain public records consistent with the State's records retention laws. Email messages generated and received with a State email account are subject to open records and records retention laws.

Request for Monthly Reimbursement/Personal Mobile Device

If an employee required to carry or authorized to use a mobile device to enhance productivity elects to use their personal mobile device, the employee will be reimbursed for voice/text only ($10) or voice and data/email usage ($25). Employees who work outside an office environment (example: some General Services Division employees) may choose to use their personal cellular phone as their work phone. In this instance, a division administrator may approve a $25 reimbursement for voice/text use only. Employees may request enrollment in MDM for reasons of convenience and receive no reimbursement; however, since there a cost associated with MDM enrollment, approval is required.

Recurring monthly reimbursements are set up to align with the fiscal year and requests must be reviewed and reapproved at the beginning of the fiscal year. Management reserves the right to adjust these reimbursement amounts at their discretion due to change in usage, position, etc.

Monthly Reimbursement Requested:

☐ $10 - Voice/Text Only
☐ $25 - Voice, Text, and Data/Email
☐ $25 - Voice/Text Only (in a position with no desk/work phone)
☐ $0 - MDM enrollment is approved for a personal cellular device, but with no reimbursement.
☐ $0 - MDM enrollment is approved for a state-owned device, no reimbursement needed.

This reimbursement is subject to applicable local, state, and federal taxes.

To assist in the installation of MDM, let us know what type of device you will be using:

Platform/Mobile Operating System	Device Ownership
☐ iOS (Apple Products) ☐ Android ☐ Windows	☐ Personal ☐ State-Owned Phone Number:

****

By signing this Mobile Device Management Agreement, I acknowledge that I have read and understand (i) the terms and conditions of the agreement and (ii) the policies and laws referenced in this agreement. I agree to comply with these laws and policies.

USER/Employee:

Signature: _____ Date: _____

Print Name: _____ Employee ID: _____

Office Location: _____ Program: _____

SUPERVISOR

Signature: _____ Date: _____

Print Name: _____

ACCOUNTING

Org/Fund/Sub Class to Charge for Monthly Recurring Expense: _____

AGENCY SECURITY OFFICER

Signature: _____ Date: _____

Print Name: _____

Once completed and all signatures are obtained, agency security officer will submit this request to the OPD Central Services Office for processing. Recurring monthly reimbursements are set up through the end of the fiscal year and must be reapproved and renewed annually.

Central Services Office Use Only:

Reimbursement timeframe: _____ to _____ Entered by: _____

Notes: _____